

# Machine Learning Based Detection Model With Human Interactions In Online Sequences

<sup>1</sup>Satyajee Srivastava, <sup>2</sup>R.V.V.S.V. Prasad, <sup>3</sup>Dr.B. YUVARAJ, <sup>4</sup>Dr. SHARADA K A, <sup>5</sup>Dr. Suresh.G

<sup>1</sup>Department of Computer Science & Engineering, School of Engineering & Technology, Manav Rachna International Institute of Research & Studies (Deemed to be University), Faridabad, Haryana, India, Orchid <https://orcid.org/0000-0001-5791-1540>

<sup>2</sup>Department of Information Technology, Swarnandhra College of Engineering & Technology, Narsapur

<sup>3</sup>Professor, Department of Artificial Intelligence and Machine Learning, Kings Engineering College Sriperumbudur, Chennai - 602117

<sup>4</sup>Professor, Department of Computer Science and Engineering, HKBK College of Engineering, Affiliated to Visveswaraya Technological University, Bengaluru -560045 Karnataka, India

<sup>5</sup>Professor, Mathematics, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College Avadi, Chennai 600062, Orcid id: 0000-0001-6453-0666

**EMAIL:** [drsatyajee@gmail.com](mailto:drsatyajee@gmail.com)<sup>1</sup>, [ramayanam.prasad@gmail.com](mailto:ramayanam.prasad@gmail.com)<sup>2</sup>, [byuvarajb@gmail.com](mailto:byuvarajb@gmail.com)<sup>3</sup>, [gs21081976@gmail.com](mailto:gs21081976@gmail.com)<sup>4</sup>, [sharada.cs@hkbk.edu.in](mailto:sharada.cs@hkbk.edu.in)<sup>5</sup>

---

## ABSTRACT

*Online shops are habitually designated by proficient lawbreakers (PMUs), who deliberately leave terrible surveys and unfortunate evaluations on their bought things to compromise the venders with illegal additions. PMUs are difficult to recognize since they utilize concealing strategies to take on the appearance of ordinary clients. There are three explicit issues for PMU recognizable proof. Professional criminals do not engage in any unusual or illegal activities and conceal themselves through the use of disguises. Therefore, conventional exception ID frameworks are puzzled because of their veiling measures. PMU identification is a multimodal challenge because the PMU detection system should incorporate all ratings and reviews. Since there are no publicly accessible datasets that include characteristics for professional fake users, PMU detection is a computational task that cannot be supervised.*

**Keywords:** *Autonomous learning, malicious professionals, recommendation systems, and metric learning*

---

## INTRODUCTION

Web based business behemoths like Amazon, notwithstanding, Jingdong as and Alibaba have flourished with the progression of Web mechanical advances, where huge number of electronic retailers create gigantic wealth by selling products on sites [1]. Consistently, billions of exchanges occur among retailers and clients [2]. Online retailers frequently permit customers (alluded to as "clients") to compose assessments and give evaluations on wares (alluded to as "things") to further develop their internet purchasing experience. To adjust the interests of traders and clients, internet business stages punish retailers who get a significant number of surveys that are negative and unfortunate client evaluations [3]. This criticism strategy has been shown to be proficient in essentially a wide range of online retailers.

Practically speaking, in any case, a few loathsome clients (MU) utilize this type of criticism to create unlawful additions [4, 5]. For example, these deceitful clients deliberately post terrible assessments and unfortunate evaluations of the products they consume without respect for the nature of the items. Then they coerce the electronic retailers to acquire unlawful additions; in any case, they leave extra regrettable criticisms, defrauding web based business sites to hurt the gadgets retailers and misdirect normal shoppers about the items in ideas. Subsequently, noxious clients harm the authenticity of web based business. Besides, their unfavorable evaluations will confound frameworks that suggest things (cooperative sifting based models [6, 7] or revolved around satisfied models [8, 9], bringing about a tumultuous positioning for standard clients, frequently known as pushing attacks [8, 9].

To settle the previously mentioned challenges, web based business associations normally use measurement exception ID or peddling attack recognition techniques [10-12] to find MUs, i.e., finding objective clients that reliably offer negative or unfortunate evaluations. These identifying models, notwithstanding, have specific limits: First, these models approach the subject just according to a perspective of system, disregarding genuine occasions. Most recognition models, for instance, disregard the way that specific expertly malignant clients (PMUs) can utilize hiding procedures to avoid location; second, they normally center around sifting either fake appraisals to further develop calculations for suggestion or unfortunate input for content-based models, and this don't think about the two assessments and evaluations. Subsequently, these sorts of models must be utilized in restricted settings in recommender frameworks.

Proficient false clients (PMU), rather than malevolent clients, frequently utilize one of the two covering strategies to sidestep current recognitions: 1) They present a decent evaluating yet regrettable criticism to forestall giving an excessive number of unfortunate appraisals. Along these lines, advertisers can deceive a potential client who is perusing this survey and picking the decision about whether to buy this thing. 2) to keep away from such a large number of terrible surveys, they give a horrible score yet an ideal survey. They might explain to the discovery of exceptions that their connections are "disoperational" along these lines. Proficient destructive clients can take on the appearance of typical clients utilizing the two strategies depicted previously.

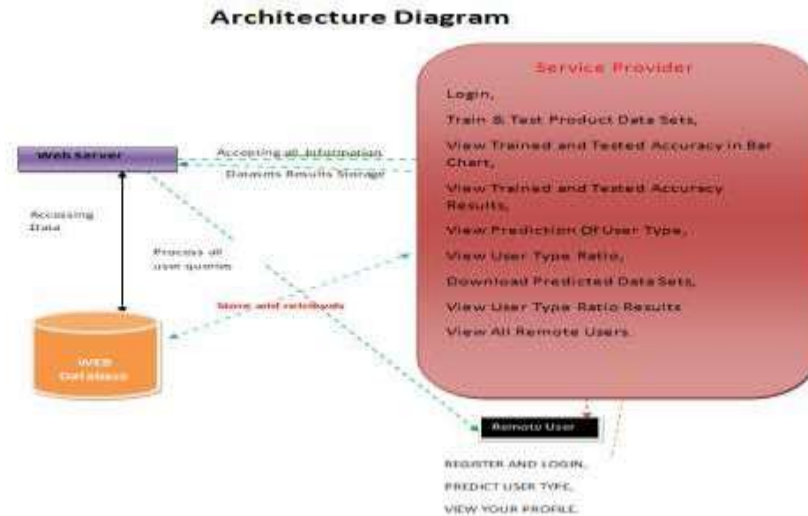
There are three main points of contention in recommender frameworks for distinguishing PMUs: 1) PMUs use veiling strategies to camouflage themselves as typical clients, making them harder to recognize. 2) Identifying PMUs requires the examination of the two assessments and evaluations, making it a multi-modular errand. 3) On the grounds that current public datasets come up short on PMU name, this recognizable proof is a solo learning challenge. To that reason, we present MMD, an unattended diverse learning model that utilizes metric learning [13-15] to distinguish fake clients utilizing surveys and appraisals. The key of metric learning is to utilize different measurements (like the separation from Euclidean or different measurements) to portray the connections between things [16, 17]. MMD at first does client profiling utilizing audits and evaluations utilizing Higher Double Consideration RNN (HDAN) [18]. Then, at that point, on this imminent set, we utilize a solo estimation learning-based grouping calculation to assign proficient hurtful clients. Specifically, we utilize the consideration cycle in estimation figuring out how to work on the model. Tests are run on four functional datasets: Amazon, Cry, the Chinese site Tao and Jingdong. The discoveries demonstrate the way that our proposed arrangement can deal with the issue of unaided vindictive client recognition. Moreover, by involving MMD as a preprocessing stage, the exhibition of bleeding edge recommender models might be gotten to the next level.

The significant commitments are summed up here.

This is the main work zeroing in on tackling the expert malignant client identification issue using the two clients' evaluations and surveys to upgrade the best in class recommender frameworks.

1. Using the changed RNN alongside consideration measurements based bunching, an original complex unstructured technique MMD-is recommended to recognize talented destructive clients.

2. Numerous tests on four true internet shopping datasets are done to approve our recommended strategy. Besides, by barring proficient hurtful individuals, different state of the art models are moved along



**Figure 1: Architecture of Store and Retrievals**

### PROPOSED Strategy AND Calculations

This exploration centers around settling the master malignant client recognizable proof issue by using both client assessments and evaluations to further develop cutting edge recommender frameworks. With a changed RNN alongside consideration metric learning-based gathering, a novel multi-modular unstructured strategy MMD-is recommended to distinguish proficient unsafe clients. Broad tests are done on four genuine web based business datasets to approve our recommended strategy. Moreover, certain state of the art models are improved by screening proficient hurtful people. The calculations recorded beneath are planned to work on the model.

#### Choice tree classifiers

Classifiers in light of choice trees have been used effectively in a great many applications. The ability to catch subjective dynamic comprehension in view of given information is their most fundamental characteristic. Preparing sets can be utilized to build a choice tree. The cycle for such age in view of an assortment of items (S), every one of which has a place with one of the classes C1, C2,..., Ck is as per the following:

Stage 1: On the off chance that the items in S are all individuals from a similar class, say Ci, choose if the tree for S contains a leaf named with this class.

Stage 2. In any case, believe T to be any test with potential outcomes O1, O2,..., On. Since every thing in S has just a single conceivable result for T, the test partitions S into subsets S1, S2,... Sn.

#### Angle supporting

Helping slopes is a fake learning approach that is usually utilized in classes and relapse applications. It returns a model for expectation as an assortment of feeble models for expectation, normally choice trees.[1][2] When a tree of decisions is utilized as the powerless understudy, the subsequent technique is known as slope helped trees, and it frequently beats the irregular woodland approach. A inclination supported backwoods model is built in similar stage-wise way as past helping strategies, however it broadens different methodologies by empowering improvement of any differentiable misfortune capability.

#### K-Closest Neighbors (KNN)

A straightforward yet solid grouping method that characterizes objects in view of their similitude.

- Non-parametric sluggish guidance doesn't "learn" until a test example is given.
- At the point when we get new information to order,
- we search for the K-closest information.

#### Model

- Guidance the informational index contains k-nearest shows in the space of highlights room implies the space with characterization factors (non-metric factors)
- Learning in light of circumstances, and in this way is powerful lethargically

- Since events extremely near a given information vector for test or guaging may find opportunity to show up in a preparation the informational collection.

### Calculated relapse Classifiers

The relationship among a reliant variable with a class and a gathering of free (illustrative) factors is researched utilizing strategic relapse investigation. Whenever the variable of interest has only two qualities, including 0 and 1 or Yes as well as No, the strategic relapse strategy is used. At the point when the reliant variable contains at least three particular qualities, for example, Drew in, Single, Separated, or Bereaved, the term strategic relapse with multinomial coefficients is utilized. Albeit the sorts of information used for the reliant part contrasts from that of a few relapses, the strategy's commonsense application is indistinguishable.

As a device for examining straight out reaction factors, calculated relapse joins with discriminant relapse. Numerous analysts accept that strategic displaying is more versatile and reasonable for demonstrating most of situations than discriminant examination. This is on the grounds that, dissimilar to discriminant investigation, the calculated relapse technique doesn't need that the factors that are independent are routinely disseminated.

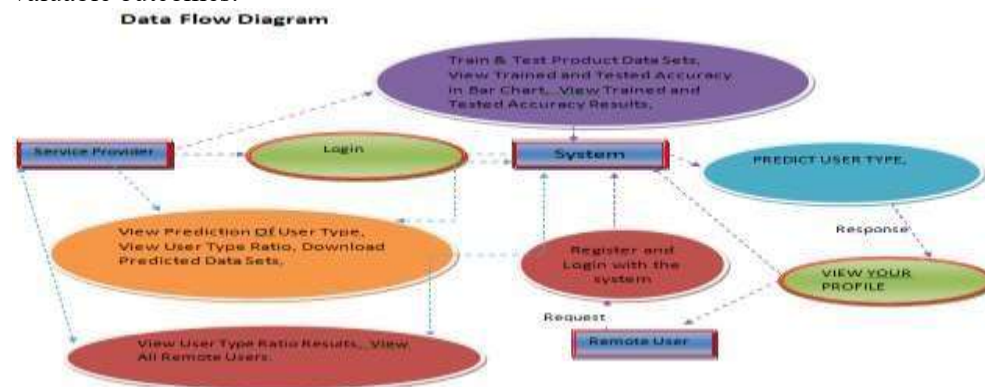
On both numeric and subjective free factors, this program processes paired calculated and multinomial strategic relapse. It gives data on the model to relapse as well as nature of fit, chances extents certainty cutoff points, likelihood, and abnormality.

It runs an intensive remaining investigation, giving indicative buildup reports and outlines. It might look for the ideal relapse structure with the least factors that are free utilizing a variable that is autonomous subset choice hunt. It gives certainty spans on expected results as well as ROC bends to help with deciding the proper classification limit. It assists you with really looking at your outcomes by ordering lines that were not used all through the concentrate consequently.

### Bayes' hypothesis

The guileless bayes method is a kind of regulated discovering that depends on a basic speculation: the presence (or nonappearance) of a specific trait of a class is free to the presence (or vanishing) of extra qualities.

In any case, it seems to be solid and effective. Its viability is identical to that of other controlled learning draws near. A few clarifications have been recommended in the writing. In this example, we will zero in on an explanation in light of illustrative predisposition. The guileless bayes classifier, similar to the straight discriminant model, strategic relapse, or a direct SVM (support vector machine), is a direct classifier. The thing that matters is in the strategy used to appraise the classifier's boundaries (the learning predisposition). While a classifier in light of Gullible Bayes is usually utilized in research, not broadly utilized by experts want valuable outcomes.



**Figure 2: Data Flow Diagram of the Service Provider**

As a result, we show the results of the most common way of learning in an alternate organization. The classifier is less complex to understand, so its organization is rearranged. We cover a few hypothetical components of the Bayesian classifier in the main part of this illustration. The technique is then tried on a dataset utilizing Tanagra. The gained discoveries (model boundaries) are contrasted with those acquired utilizing elective

straight systems like calculated relapse, direct discriminant examination, and direct SVM. The discoveries are genuinely predictable, as may be obvious. This altogether makes sense of the technique's predominant progress interestingly, for other people. In the subsequent area, we utilize a few devices to a similar data set.

### **Arbitrary Backwoods**

Irregular timberland models, otherwise called irregular decision woodlands, are a group based technique for learning for relapse, characterization, and different issues that works by building countless choice trees during preparing. For arrangement issues, the arbitrary woods result is the class picked by most of trees. The mean or normal gauge of all of the trees is accommodated relapse assignments. Randomized choice backwoods address choice trees' propensity to overfit their preparation set. Irregular woodlands reliably perform choice trees as a rule, albeit the accuracy they produce is lower than that of inclination improved trees. In any case, information characteristics can affect execution.

Tin Kam Ho[1] fostered the primary strategy for irregular decision timberlands in 1995, using the arbitrary space method, which Ho characterized as a method for applying Eugene Kleinberg's "stochastic separate" way to deal with characterization.

Leo Breiman that Adele Cutler made an extension of the technique and enlisted the brand name "Irregular Timberlands" in 2006 (which is currently held by Minitab, Inc.). The development mixes Breiman's "sacking" idea with irregular component choice, at first recommended by Ho[1] and afterward independently by Amit and Geman[13], to make a bunch of choice chains with directed change.

Irregular backwoods are normally utilized in associations as "blackbox" models since they produce great forecasts all through a wide assortment of information with little planning.

### **SVM**

A differentiator AI approach in order issues attempts to find a capability with discriminant properties that can appropriately anticipate names for as of late gained occasions in view of an independent and similarly dispersed (iid) preparing dataset. As opposed to generative AI procedures, which need the development of restrictive probabilistic installments, a discriminant order capability takes a snippet of data  $x$  and designates it to one of the few classes that include the characterization work. Discriminant calculations need less computer processor assets as well as less preparation information than created approaches, which are for the most part used when expectation requires exception recognizable proof. This is particularly valid for a multivariate component space and when simply back probabilities are required. Learning a characterization framework is mathematically similar to deciding the condition for a heterogeneous surface.

SVM is a classifier approach, and on the grounds that it settle the curved improvement issue systematically, it generally gives an indistinguishable ideal hyperplane boundary — in contrast to hereditary calculations, otherwise called GAs, or perceptrons, which are both normally utilized in AI for characterization. Answers for perceptrons are unequivocally dependent on the startup and ending models. Preparing produces remarkably indicated SVM boundaries for the model for a specific preparation set for a specific bit that interprets the information from the space utilized for contribution to the area of elements, while each of the perceptron and GA AI models are unmistakable each time teaching is initialised. The objective of GAs and discernments is basically to diminish mistake in the wake of preparing, which will bring about various hyperplanes matching this models.

## **RESULTS AND DISCUSSION**

### **AI for Grouping**

The key for this distinguishing proof is knowing how to differentiate between proficient unsafe clients and ordinary clients. With bunching, the conspicuous idea is to amplify the distance among malignant and normal clients. We utilize Metric Learning in this review, an unmistakable hypothesis that is regularly utilized

in bunching, position and acknowledgment of pictures. The measurement learning worldview means to gauge a proper "distance" between things to evaluate their associations [21]. Consider the accompanying distance metric cluster A:

$$d_A(p_j, p_k) = \|p_j - p_k\|_A = \sqrt{(p_j - p_k)^T c^2 A (p_j - p_k)} \quad (1)$$

Where  $j, k \in U$  is an ordinary boundary,  $p_j$  and  $p_k$  are covered up vectors for  $j, k$ , and  $c$  is a typical boundary. When  $A = 0$ , framework A turns into a measurement (it satisfies non-cynicism and the triangle condition in idle space). Metric learning expects to become familiar with a metric where the different pivot are given unique "loads" to do grouping. An essential thought for making a measures for an ideal meter is to limit the partition  $d_A(j, k)$  if  $j, k$  are in indistinguishable client subgroup  $S$  (which infers  $j, k$  should fit nearer under the models of the metric lattices  $A$ ), and afterward add extra imperatives to ensure  $A$  doesn't push the client set into an area known as a "metric". This outcomes in an enhancement trouble.

$$\begin{aligned} \min_A \quad & \sum_{j, k \in S} d_A(p_j, p_k); \\ \text{s.t.} \quad & \sum_{j, k \in (U-S)} d_A(p_j, p_k) \geq c, A \succ 0. \end{aligned} \quad (2)$$

### Model Enhancement

In close by limiting the LMLC abstract misfortune capability, we investigate boundary limitations to make MLC less powerless to negative testing. Expect that the model sources of info contain the metric lattices  $A_n$  and  $A_n$  and the engaged vector set  $t$ . Subsequently, we characterize the MLC improvement point as:

$$\Theta^* = \arg\min_{\Theta} L_{MLC} + \|\Theta\|_2 \quad (3)$$

In which  $\|\cdot\|_2$  is the F2-standard regularization. In this methodology, we all the while learn metric lattice  $A$ , which is alongside the consideration vector set  $t$ . It ought to be noticed that in the real world, PMU just records for a little level of clients (practically 10%). We should harmony the loads of named (PMUs) and unlabeled (ordinary clients), in this manner ought to be more than 0.5.

### Learning Calculation

By limiting Eq, the model boundaries are refreshed at this stage. This goal capability shows estimation  $A_n$  and consideration weighting  $W_t$  Eq. simultaneously. A standard minimization issue might be tackled utilizing the strategy for slope plummet. We explicitly lead a change step for every one of the boundaries in question:

$$\Theta = \Theta - \eta dL_{MLC}/d\Theta \quad (4)$$

At the point when some auto-versatile Gd models are utilized, where  $\eta = A, W_t$  implies the model's learning rate, that is boundary subordinate. Adagrad [27] was picked as our SGD calculation in the model we proposed. We can: 1) example the named proficient destructive clients every now and again to create extra examples (for each recognized proficient hurtful client, pick 5 to 10 unlabelled standard clients to obtain the measurement); and 2) increment the significance of labeled clients. We can approve the exhibition by following the profit from a holdout control dataset.

Regarding the consecutive plan of MMD, the general worldly intricacy ought to be diminished.

$$O_{MMD} = O(n \log n) + O(nd^2) + O(p \log p + k^2) \quad (5)$$

### Algorithm for MMD Model

Expert Dangerous User Identification Using an Attention Monitoring Learning Algorithm (MMD)



Customers' feedback for HDAN, MUP, and MLC U, objects I, rate R, ratings V, attitude gap  $\_g$ , identification cutoff  $\_mu$ , rate for learning  $\_O$ .

As an output AL distance the metric system, umu, professional damaging users.

MMD is, as far as we know, the first system to incorporate HDAN plus metrics teaching for PMU recognition in suggestions plus feedback and assessments. The MMD Model is as follows:

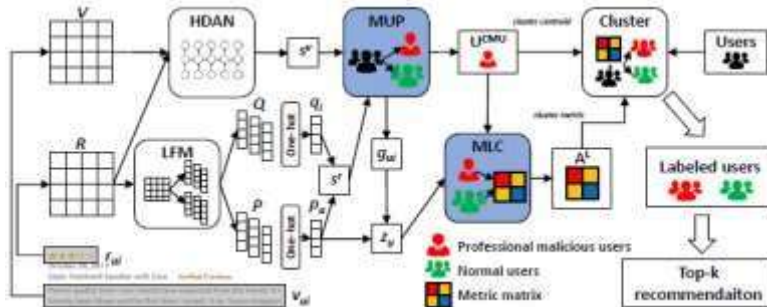


Figure 3: Professional Malicious User Detection Model



Figure 4: Machine Learning in Recommender Systems



Figure 5: Login Details of Service Provider

Figure 6: Registration Details

USER NAME	EMAIL	Gender	Address	Mob No	Country	State	City
Govind	Govind133@gmail.com	Male	#892,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore
Manjunath	imkumarju13@gmail.com	Male	#892,4th Cross,Rajajinagar	9535866270	India	Karnataka	Bangalore

Figure 7: Location Identification of Remote Users

Figure 8: Prediction of Malicious Users



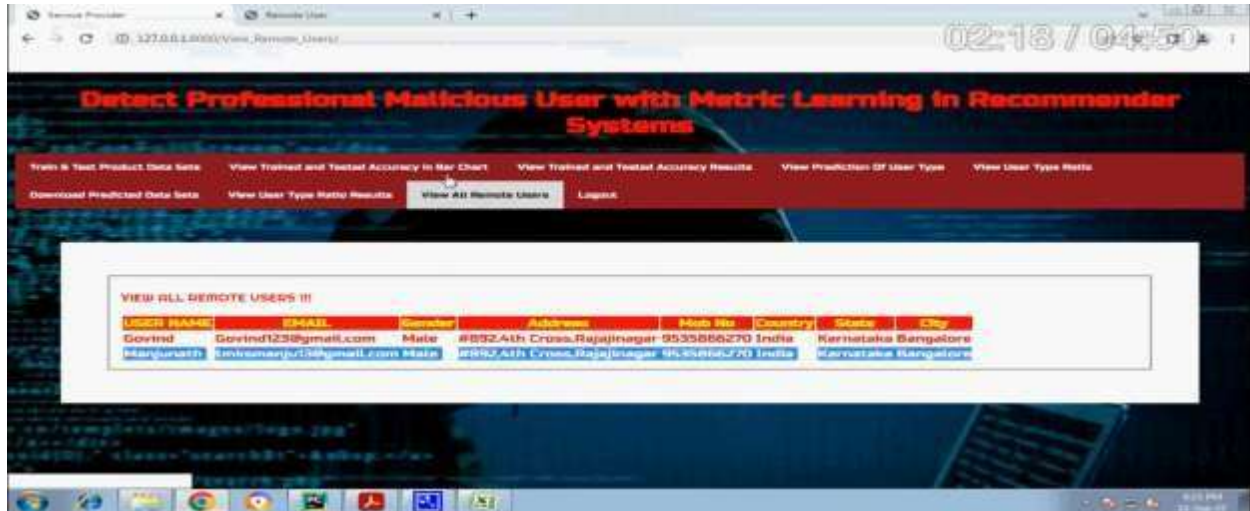


Figure 9: Identification of Remote Users

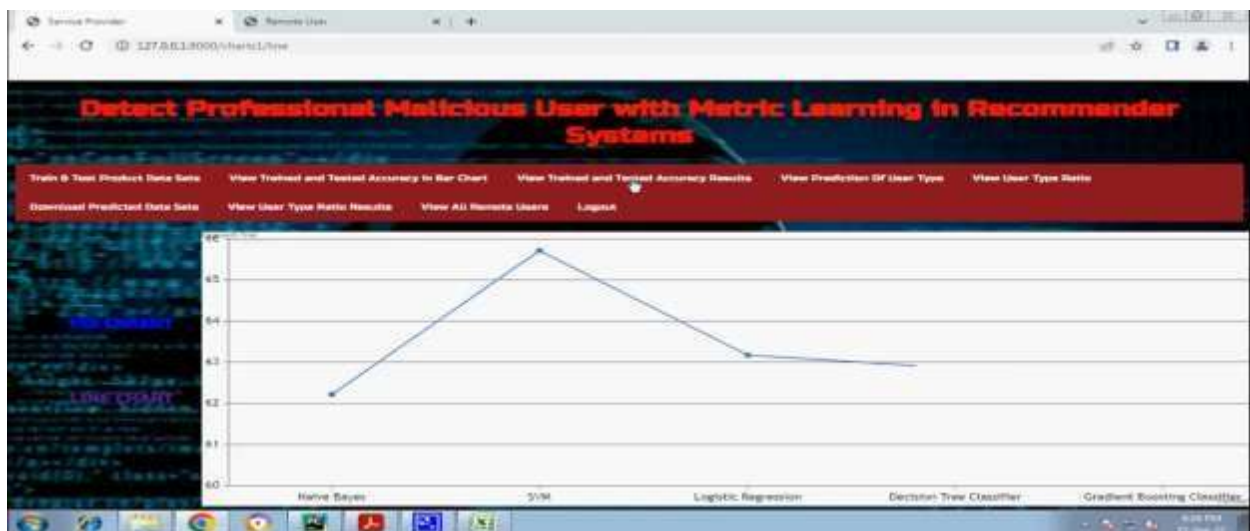


Figure 10: Analysis of Naïve Bayes, SVM, Logistic Regression, Decision Tree Classifier and Gradient Boosting Classifier

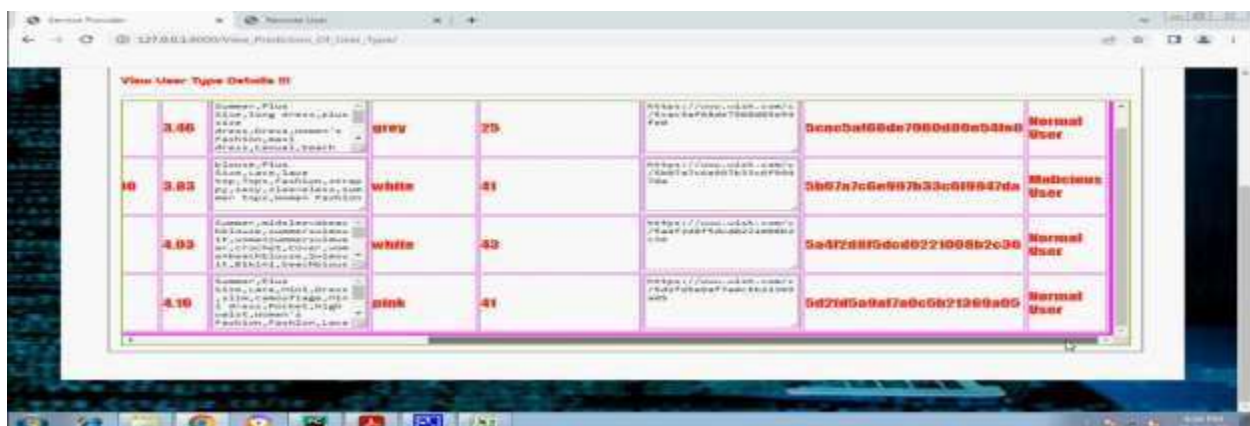
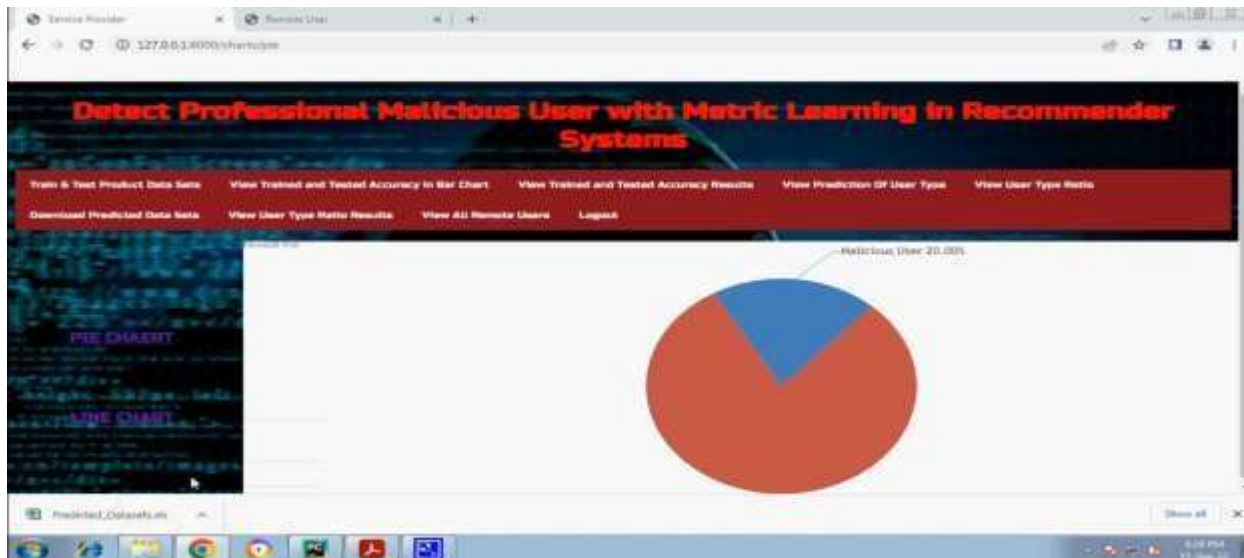


Figure 11: User Details

**Figure 12: Prediction of Malicious User Type**



**Figure 13: Analysis of Malicious users with online Sequences**

## CONCLUSION

In this study, professional nefarious users (PMUs) were classified as those that provide false feedback in order to mislead normal users, harm recommender systems, and profit illegally. Due to professional masking tactics, typical outlier findings could not be used in the recommendation mechanism region to identify these professional harmful individuals. MMD, a novel unsupervised multimodal instruction model, was created to address an expert unauthorized user detection issue. MMD discovered a suitable measure for clustering users and identified professional malevolent users. In conclusion, MMD is an umbrella strategy that may not only identify the competent harmful individuals explored in the present investigation, but also provide a general base for unwanted person detections. MMD may be instructive in recognising the emotional of dissatisfied with titles that are unhappy and happy using additional data such as image, and video, or sound, which has a potential future in countering varied masking strategies in many businesses. Furthermore, we will incorporate audiovisual data into our model and consider the impact of factors such as spending period of time, press releases, and other initiatives. Finally, we want to create an online professionals risky user identification model that requires use of recent advances in human-machine interactions.

**REFERENCES**

- [1] C. G. Traver and K. C. Laudon, *E-commerce: business, technology, society*. Pearson Prentice Hall/Pearson Education, 2008.
- [2] B. Rutherford, A. Dagher, M. Wiseman, D. J. M. C. Paie, J.-P. E. Rans, F. Ates, and J. Wankmueller, "Customer authentication in e-commerce transactions," Dec. 6 2016, uS Patent 9,514,458.
- [3] S. Akter and S. F. Wamba, "Big data analytics in e-commerce: a systematic review and agenda for future research," *Electronic Markets*, vol. 26, no. 2, pp. 173–194, 2016.
- [4] M. Si and Q. Li, "Shilling attacks against collaborative recommender systems: a review," *Artificial Intelligence Review*, pp. 1–29, 2018.
- [5] Y. Cai and D. Zhu, "Trustworthy and profit: A new value-based neighbor selection method in recommender systems under shilling attacks," *Decision Support Systems*, vol. 124, p. 113112, 2019.
- [6] X. He, L. Liao, H. Zhang, L. Nie, X. Hu, and T.-S. Chua, "Neural collaborative filtering," in *Proceedings of the 26th international conference on world wide web*. International World Wide Web Conferences Steering Committee, 2017, pp. 173–182.
- [7] J. Su, "Content based recommendation system," Jan. 5 2016, uS Patent 9,230,212.
- [8] W. Zhou, J. Wen, Q. Xiong, M. Gao, and J. Zeng, "Svm-tia a shilling attack detection method based on svm and target item analysis in recommender systems," *Neurocomputing*, vol. 210, pp. 197–205, 2016.
- [9] Y. Xu and F. Zhang, "Detecting shilling attacks in social recommender systems based on time series analysis and trust features," *Knowledge-Based Systems*, vol. 178, pp. 25–47, 2019.
- [10] S. K. Kwak and J. H. Kim, "Statistical data preparation: management of missing values and outliers," *Korean journal of anesthesiology*, vol. 70, no. 4, p. 407, 2017.
- [11] R. A. Maronna, R. D. Martin, V. J. Yohai, and M. Salibi'an-Barrera, *Robust statistics: theory and methods (with R)*. John Wiley & Sons, 2019.
- [12] C. Tong, X. Yin, J. Li, T. Zhu, R. Lv, L. Sun, and J. J. Rodrigues, "A shilling attack detector based on convolutional neural network for collaborative recommender system in social aware network," *The Computer Journal*, vol. 61, no. 7, pp. 949–958, 2018.
- [13] D. Wang and X. Tan, "Robust distance metric learning via bayesian inference," *IEEE Transactions on Image Processing*, vol. 27, no. 3, pp. 1542–1553, 2018.
- [14] X. Sui, E. L. Xu, X. Qian, and T. Liu, "Convex clustering with metric learning," *Pattern Recognition*, vol. 81, 2018.
- [15] W. Zuo, F. Wang, D. Zhang, L. Lin, Y. Huang, D. Meng, and L. Zhang, "Distance metric learning via iterated support vector machines," *IEEE Transactions on Image Processing*, vol. PP, no. 99, pp. 1–1, 2017.
- [16] H. J. Ye, D. C. Zhan, and Y. Jiang, "Fast generalization rates for distance metric learning," *Machine Learning*, pp. 1–29, 2018.
- [17] J. Li, A. J. Ma, and P. C. Yuen, "Semi-supervised region metric learning for person re-identification," *International Journal of Computer Vision*, vol. 126, no. 8, pp. 855–874, 2018.
- [18] Y. Xu, Y. Yang, J. Han, E. Wang, F. Zhuang, J. Yang, and H. Xiong, "Neuo: Exploiting the sentimental bias between ratings and reviews with neural networks," *Neural Networks*, vol. 111, pp. 77–88, 2019.
- [19] Y. Xu, Y. Yang, J. Han, E. Wang, J. Ming, and H. Xiong, "Slandorous user detection with modified recurrent neural networks in recommender system," *Information Sciences*, vol. 505, pp. 265–281, 2019.
- [20] Z. Yang, D. Yang, C. Dyer, X. He, A. Smola, and E. Hovy, "Hierarchical attention networks for document classification," *Proceedings of the 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, pp. 1480–1489, 2016.
- [21] E. P. Xing, M. I. Jordan, S. J. Russell, and A. Y. Ng, "Distance metric learning with application to clustering with side-information," in *Advances in neural information processing systems*, 2003, pp. 521–528.
- [22] X. He, H. Zhang, M.-Y. Kan, and T.-S. Chua, "Fast matrix factorization for online recommendation with implicit feedback," in *Proceedings of the 39<sup>th</sup> International ACM SIGIR conference on Research and Development in Information Retrieval*. ACM, 2016, pp. 549–558.
- [23] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in *Advances in neural information processing systems*, 2017, pp. 5998–6008.
- [24] M.-T. Luong, H. Pham, and C. D. Manning, "Effective approaches to attention-based neural machine translation," *arXiv preprint arXiv:1508.04025*, 2015.
- [25] X. He, J. Tang, X. Du, R. Hong, T. Ren, and T.-S. Chua, "Fast matrix factorization with non-uniform weights on missing data," *IEEE transactions on neural networks and learning systems*, 2019.
- [26] S. Rendle, C. Freudenthaler, Z. Gantner, and L. Schmidt-Thieme, "Bpr: Bayesian personalized ranking from implicit feedback," in *Proceedings of the twenty-fifth conference on uncertainty in artificial intelligence*. AUAI Press, 2009, pp. 452–461.
- [27] J. Duchi, E. Hazan, and Y. Singer, "Adaptive subgradient methods for online learning and stochastic optimization," *Journal of Machine Learning Research*, vol. 12, no. Jul, pp. 2121–2159, 2011.
- [28] R. Senthamil Selvan "An Optimized Dual Temporal Gated Multi-Graph Convolution Network Based Denial of Service Attack Distribution Detection in Cloud Computing" by *International Journal of Bio-Inspired Computation*, ISSN: 1758-0374, DOI: 10.1504/IJBIC.2024.10069266 (Inderscience-SCI Indexed)